ANAND GURU

Senior Security Analyst

+1 9876543210
anandguru.in@gmail.com
www.linkedin.com/in/anand-guru

AREAS OF INTEREST

- Threat Hunting
- Threat Intelligence
- SOAR (IR Automation)
- Malware Analysis
- Forensics

CERTIFICATIONS

- EC Council – Certified Ethical Hacker (CEH)
- Splunk User Certified

EXPERIENCE

Company Name
Designation
Apr 2019 – Till Date

Company Name
Designation
Apr 2019 – Till Date

EDUCATION

BE in Computer Science from ABC University | 2011

PROFESSIONAL SUMMARY

- 4+ years of experience in Cybersecurity with focus on Security Operations.
- Strong hands-on experience in security management tools like IBM QRadar and Splunk including log source on-boarding, creating reports and dashboards, writing custom parsers and correlation rules
- Knowledge on advance capabilities like Threat Hunting and Malware Analysis
- Exposure to regulatory compliance like PCI-DSS and ISO 27001.
- Good experience in working/communicating with cross-functional IT infrastructure teams like network, system, database, application, security to build and manage effective security operations.
- Capable of independently learning new technology by utilizing available documentation and vendor support resources.
- Strong analytical and problem solving skills as needed to perform the job of a SOC analyst.

TOOL EXPOSURE

SIEM	: IBM QRadar, Splunk
End point Security	: McAfee ePO
Network Security	: PaloAlto, Proofpoint, Websense
VA	: Nessus
Analysis Tools	: IPVoid, VirusTotal, SysInternals, Wireshark
Ticketing Tool	: Service Now

Work in Detail

Company Name
Designation
Apr 2019 – Till Date

- Alert monitoring and Incident response using Splunk SIEM.
- Analyze threats by taking the events from Firewalls, Endpoints, Servers, IDS/IPS etc. and identify a false positive and a true positive.
- Perform a detailed analysis on the threats that are triggered and suspected to be true positives.
- Investigating incidents, remediation, tracking and follow-up for incident closure with concerned teams and stakeholders.
- Interact with Security Owners/Stakeholders, L2 & L3 Level infrastructure teams for remediation of security alerts
- Generation & formatting of reports for Nessus Vulnerability scans performed.
- Weekly walk-through of latest attack trend, IOCs and TTPs to the team.
- Engage with vendor support to troubleshoot issues with SIEM platform.
- Preparation of Security Operations Handbook.

Company Name
Designation
Apr 2016 – Apr 2019

- Monitoring Security alerts generated by SIEM.
- Analyzing SIEM alerts by following runbooks and using various tools.
- Generating tickets for validating incidents.
- Assist in identifying Root Causes of incidents and follow-up with SMEs for incident closure.
- Assist the team lead in generating weekly report.
- Documentation of alerts.
- Draft Shift Handover.